GUIDE TO OPERATIONAL SUPPORT SERVICES

TABLE OF CONTENTS

GUIDE TO OPERATIONAL SUPPORT SERVICES

PREFACE

The objective of this monograph is to provide a concise, functional description of the information operations (IO) support services available from the Army LIWA to a land component command(er) responsible for garrison, exercise, test and evaluation, experimental or contingency activities embracing the full range of IO in Army operations. The LIWA's support capabilities can be extended to operational as well as tactical operations. For field support operations, the diversified capabilities of the LIWA are appropriate for applications at the echelon of the requesting Army forces (ARFOR) component of a U. S. unified command CINC-designated Joint Task Force (JTF). However, LIWA elements are equally applicable for employment with Army elements without JTF command and control. In some instances, LIWA contingents have deployed in direct support roles for the ARFOR and its higher echelons, including coalition operations.

With its Information Dominance Center (IDC), the LIWA is capable of providing split-based, virtual support continuously to its field elements and their supported commands, worldwide, through its expansive telecommunications and computer networks. The IDC has direct communications access to Government, coalition and non-Government agencies and activities capable of supporting IO activities at any level of commitment.

This document was developed by
EWA Information and Infrastructure Technologies (IIT), Inc.
for
U. S. Army Land Information Warfare Activity
8825 Beulah Street, Fort Belvoir VA 22060-5246
under Contract Number DASC01-98-D-003

1 May 2000

I. PURPOSE

The purpose of this guide is to introduce the several operational roles of the U. S. Army Land Information Warfare Activity (LIWA) in fulfilling its charter as the *operational focal point* for the integration of ***information operations (IO)*** in the Army.

II. THE LIWA ROLE IN INFORMATION OPERATIONS

The LIWA was organized in 1995 to integrate IO into every aspect of Army operations. The organization assists in planning, synchronizing, executing and assessing IO for worldwide Army warfighting and other commanders in garrison, on field training exercises and experiments and in contingency operations. The LIWA provides and/or coordinates for the appropriate level of IO and IO-related support to Army and land component commanders (LCCs) from Army, joint Service, other (US) Government, non-Government and coalition resources, as required.

The Director, LIWA is designated (a) the commander of the Army forces component (ARFOR) of the U. S. Space Command's Joint Task Force for Computer Network Defense (JTF-CND), and (b) the functional proponent for battlefield deception in the Army.

The LIWA's base of operations is located at the Headquarters of the U. S. Army Intelligence and Security Command (INSCOM), the LIWA's parent command, at Fort Belvoir VA. From this location, the Director, LIWA administers the four operational programs in which the LIWA is continuously engaged*:* ***field support, computer emergency response, vulnerability assessment*** and ***emergency reprogramming of Army target sensors.***

A. INFORMATION DOMINANCE CENTER

The LIWA provides back-up support to 24-hour, worldwide IO activities through the INSCOM Information Dominance Center (IDC), for the most part manned by LIWA personnel. Acting as an operations center, IO intelligence analysis center and communications hub, the IDC is the focal point for all support to the LIWA's Army and joint activities. LIWA elements deployed worldwide are continuously linked to the IDC via a number of communications means, including common-user circuits, strategic communications links and dedicated satellite terminals. The IDC maintains the status of IO events worldwide and orchestrates the activities of the LIWA's deployed elements and internal supporting activities.

As an analysis center, the IDC provides dedicated support to LIWA's deployed teams and to the commands the teams serve. Tailored analytical products are generated, frequently on a quick-response basis, to meet a deployed team's immediate needs. The IDC also monitors potential trouble spots worldwide, and continuously prepares to support contingency operations with IO-related products should the need arise.

The IDC's high-capacity communications links are used to access and transmit selected information from a number of databases maintained by a number of other commands, agencies and organizations. IDC communi-cations are also used to flash computer intrusion alerts and countermeasures across the Army. IDC connectivity is ensured via TROJAN, SIPRNET, NIPRNET and secure voice/fax between deployed/detached elements of the LIWA and the LIWA base of operations. Other IDC connectivities employ the following networks and systems:

- Automated Message Handling System (AMHS)

- Global Command and Control System (GCCS)
- Joint Deployable Intelligence Support System (JDISS)
- Multi-Media Information Exchange Network (MINX)
- Multi-Mission Advanced Technical Terminal (MATT) with Generic Area Limitation Environment (GALE) Processor
- National Security Agency Network (NSANET)
- Open Source Information System (OSIS)
- Linked Operations - Intelligence Center, Europe (LOCE)

For more information on the INSCOM IDC, call DSN 235-1560 (commercial 703-706-1560).

B. OPERATIONAL PLANNING

Ideally, IO planners from the LIWA Plans Branch are brought into the planning cycle at the earliest possible point in operational plan development. Even before a LIWA element is selected and committed to an IO support mission, and as early as practicable after a request for LIWA support is approved, LIWA planners participate in the requesting command's planning process for Army or LCC exercise or contingency support.

Warfighter Exercises

Normally, in preparation for a Battle Command Training Program (BCTP) warfighter exercise, LIWA IO planners are involved with a BCTP-conducted *Warfighter Seminar*, at which all exercise player and control parties are participants. The purpose of the seminar is to develop the battlefield scenario, determine the level of support required from the LIWA, review and revise appropriate OPLANs/OPORDs to encompass IO objectives and establish the ground rules for the exercise event. The seminar takes place between D-90 and D-120 days.

At D-30, the BCTP *Ramp-Up Exercise*, with LIWA IO planners again in attendance, is scheduled at the warfighter unit to finalize planning for the exercise event. At this point, the scenario, adversary order of battle and friendly force structure are set for the event.

Joint Exercises

For joint, normally combatant command CINC-sponsored field training exercises, where an Army LCC is established or the joint command headquarters is formed around an existing Army corps/division headquarters, LIWA IO planners participate in all exercise planning conferences.

The Initial Planning Conference for joint exercises is scheduled 8-9 months ahead of the field event; the Mid-Planning Conference is set for between D-120 and D-150 days; the Final Planning Conference occurs at about D-60 days.

Contingency Operations

Real-world experience has shown that early involvement of the LIWA planners is crucial to the success of multi-disciplined IO in support of contingency operations. LIWA planners review or prepare the appropriate annexes to ARFOR/LCC OPLANS and OPORDS for command IO applications,

determine and recommend the level of LIWA support required and lay the groundwork for deployment of any LIWA contingent required.

For more information about multi-disciplined IO planning support for future operations, contact the LIWA Plans Branch at DSN 235-1067 (commercial 703-706-1067).

C. FIELD SUPPORT

The LIWA element most likely to respond to a request for IO in support of an exercise, experiment or contingency operation is a multi-disciplined, tailored ***Field Support Team (FST)***. When requested, a LIWA FST deploys in an attached (less administrative) status and provides direct support as an integral part of the supported command's IO staff. The LIWA currently provides support, in priority order, to contingency operations, ARMY XXI activities and training exercises at the echelons of corps and above; support at the levels of division and below is provided on a case-by-case basis.

FST Composition and Capabilities

The composition of the FST is based on the resident or attached IO capabilities of the supported command. The team normally is led by a Team Leader (MAJ) who acts as the spokesperson for the team and coordinates with the leadership of the supported command and other supporting elements (e. g., Vulnerability Assessment Team, if employed). For 24-hour operations, the FST could include up to ten individuals (military, Government civilian or contractor) with primary skills and experience in multi-disciplined IO planning and operations. Other disciplines that might be represented in the FST include information systems architectures; information systems security; electronic warfare (EW), operations security (OPSEC), deception, computer network attack/defense (CNA/CND), civil affairs (CA), public affairs (PA) and psychological operations (PSYOP) planning; intelligence; and multi-disciplined counter-intelligence (CI).

The FST members may be drawn entirely from the LIWA, or could be a core LIWA group augmented by other components, e. g., Army Reserve or National Guard. The FST comple-ment is also tailored to the supported commander's needs to fill any gaps in the command's staff capabilities in IO and IO-related disciplines. Individuals with specific disciplines not represented in the deployed FST complement are available by reach-back communications to the LIWA home base, and may be called forward or respond remotely from the home base, as needed.

FST Planning

The LIWA FST employs the IO planning cycle in close harmony with the Army military decision-making process (MDMP), with some noticeable differences. They stem from the need for longer lead times required for integrated, coordinated planning for the full spectrum of IO capabilities. And, (often) there is long lag time between implementation and effects determination of some IO (e. g., civil-military operations [CMO] - including PSYOP, CA and PA, and deception).

Field Support Team members' planning capabilities include advising and assisting in the following activities.

- Analyzing the commander's initial IO guidance and intent;
- IO mission analysis, developing and wargaming courses of action (COAs), building information and decision briefings and supporting synchroni-zation and coordination of IO activities; and

- Writing and reviewing plans, and conducting coordination with other component commands' IO elements, the senior joint command (if designated) IO element and other DoD/Government and non-DoD/non-Government agencies and activities.

Preparation of the Battlespace and IO

The LIWA FST coordinates multi-disciplined intelligence and other support for IO planning and execution, to include database development and maintenance. The FST provides assistance in developing input to intelligence collection plans tailored to support IO, including battle damage and combat assessments, and assisting the IO cell in acquiring essential adversary and regional intelligence information to build and maintain IO databases.

The deployed FST, attached as an integral component of the supported command staff, relies on the existing information and intelligence architectures of the command to provide the level of detailed information required to support IO planning and execution. The FST also maintains a reach-back capability with the LIWA at Ft. Belvoir for responsive, topical information retrieval and analytical support in the following areas, relative to adversary, friendly and neutral entities.

- Decision-maker identities, biases and inter-relationships,
- Identification of critical C2 and information links and nodes,
- Other key telecommunications and information systems,
- Data on adversary sensor-to-shooter links,
- Demographic data for the area of operations,
- Populace biases/pre-dispositions,
- Potential pressure points to leverage decision-maker/populace behaviors, and
- Mass media capabilities.

Targeting

Targeting in concert with IO underscores the required ***effects*** of integrating and synchronizing the lethal and non-lethal capabilities of the command. The IO/targeting synchronization requires information to enable the destruction, denial or degradation of vital C2 links and nodes at the right time and place; thus, detailed knowledge of adversary C4ISR capabilities is essential. The LIWA FST members can contribute to the targeting process by assisting in developing and refining IO synchronization and attack guidance matrices and in interpreting IO-integrated battle damage and/or combat assessment.

FST Support Requirements

The FST normally brings its own communications and automated information systems. All systems are capable of operating in a SCIF environment. The team requires workspace and access to Class "A" (or equivalent) unclassified and classified telephone service in the supported command's facility for each shift of operations. To be most effective, the FST will require supported command internet protocol (IP) addresses and continuous access to the command's internal, LAN and NIPRNET/SIPRNET during the period of operational support. Other accommodations needed for the FST include:

- Local living accommodations (including tactical facilities/services, e. g., messing, transportation);
- Local security protection for FST equipment, classified information, weapons and COMSEC material; and
- When required, local facilities, equipment and material needed to support the conduct of IO training for command personnel by the FST.

Lessons Learned in FST Operations

Experience shows that the value-added benefit of LIWA commitment to field activities is realized best when the supported command's pre-deployment activities include the LIWA as a participant from the earliest date possible. When the LIWA is provided early identification of any strengths and weaknesses in the command's staff capabilities involving the IO and IO-related disciplines, the FST can be tailored to best fit the supported command's needs. The LIWA FST role is particularly supportive when:

- Activities of the IO cell are habitually included in the command's battle rhythm;
- The LIWA FST assists in exercise or contingency scenario-building and OPLAN and OPORD development; and
- IO representation is habitually included in the command's current operations, targeting and planning efforts.

For a comprehensive discussion of the LIWA FST functions and capabilities, see the LIWA Information Operations (IO) Handbook (Draft), October 1998, and the LIWA publication IO Planning and the MDMP, 6th Edition, May 1999. Call the Chief, FST Division (DSN 221-5674/commercial 703-325-5674) at the LIWA for more information on FST support.

D. COMPUTER EMERGENCY RESPONSE

The threats to Army information and information systems have three primary objectives: compromise of information, corruption of data and disruption of operations. To protect against these threats, the Army established the ***Army Computer Emergency Response Team (ACERT)***. The ACERT provides the Army with the capability to prevent, monitor, detect and respond to automated information systems (AIS) security incidents. The ACERT leverages and integrates intelligence support and network/system management capabilities in an assertive, unified defensive IO (DIO) effort.

The ACERT is organized with an around-the-clock Coordination Center (CC) at Fort Belvoir, two Ft Belvoir-based immediate-reaction *("Blue"*) teams and four Regional CERTs (RCERTs) collocated with U. S. Army Signal Command (ASC) network operations centers (NOCs) in Hawaii, Germany, Korea and Ft Huachuca AZ. The ACERT/CC is established in the INSCOM IDC, where a 24-hour, worldwide vigil over the Army's information systems is maintained. ***The ACERT is the DA single point of contact for reporting information system security incidents and vulnerabilities and is responsible to HQDA for coordinating an appropriate response to incidents***.

In most cases of incidents affecting AIS, the affected system administrator initiates the incident report. Reports of suspected or known intrusion attempts and actual incidents are reported to the appropriate RCERT and local Army counterintelligence and law enforcement (Criminal Investigation Command) authorities. Higher-level reporting is done by the ACERT/CC, which also disseminates advisories and anti-virus software and assists commands in taking appropriate action in response to computer attacks.

When requested, an ACERT Blue Team is dispatched to assist commanders, information security managers and system administrators by providing technical support in dealing with computer incidents and intrusions. Such a team may come from the ACERT/CC or may be made up from personnel located at one of the regional locations. ACERT assistance includes post-attack system restoration, when required.

The ACERT/CC implements HQDA tasking to the ASC or other appropriate command(s) for execution, and acts as the Army interface point for exchanging reports of computer incidents and intrusions with other Service, joint and National agencies and activities. The LIWA ACERT is also

designated the Army Force (ARFOR) Component of the CINCUSSPACECOM Joint Task Force for Computer Network Defense (JTF-CND) in support of the unified JCS effort to plan for and conduct the defense of DoD-wide information systems and networks. In addition, the ACERT/CC is the functional manager for C2-Protect tools and the C2-Protect Toolbox for the Army and maintains a repository of security tools to make available as appropriate.

Computer Defense Assistance

The Computer Defense Assistance Program (CDAP) of the ACERT provides requesting "sustaining base" activities and commands with identification, verification, analysis and reporting of their information systems' vulnerabilities. The CDAP also offers technical support to mitigate these vulnerabilities. The goal of the CDAP is to prevent unauthorized access to Army computer systems by identifying points of unauthorized access, assessing the depth and degree of potential compromise and recommending methods, techniques and configuration modifications needed to secure the threatened systems.

The CDAP event process is organized and structured in phases (see Figure 1, below) to provide layers of evaluation and build on the preceding phase/phases. This phased approach allows the requesting unit commander or activity to *customize* the program to meet unit needs and expectations. Phases 1 and 2 provide authorization and information about the target information systems network or sub-net and establish assessment execution procedures. Phases 3 and 4 identify suspected systems' vulnerabilities; Phases 5 and 6 penetrate vulnerable network systems to verify suspected vulnerabilities and analyze network protective capabilities. Phase 7 provides technical support to assist in mitigating these vulnerabilities. Phase 8 provides a final report to the requesting command/activity. *The contents of this report are considered to be "sensitive" and will be disseminated only by the requesting command/activity.*

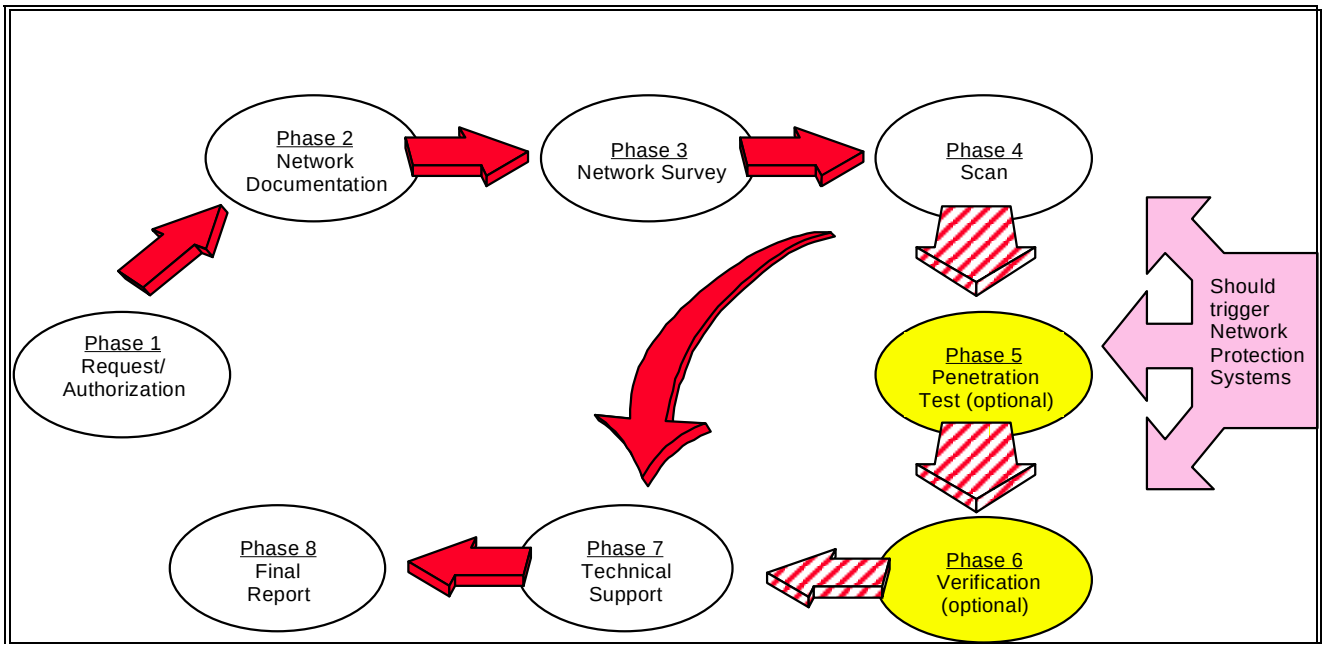

Figure 1. CDAP Process

CDAP Team Composition and Capabilities

The ACERT CDAP team has the capability to perform assessments by either on-site or

remote means; however, the preferred method for performing command/activity vulnerability assessments involves remote accessing from the LIWA home base at Ft. Belvoir, VA, whenever possible, to present a realistic hacker/intruder attack. When dispatched, a typical ACERT/CDAP team consists of one or two people, usually led by a DA civilian who acts as the spokesperson for the team and coordinates with the leadership of the assessed activity/installation.

Team personnel are trained in network and information system security for the different operating systems in the Army inventory. They are provided with appropriate portable laptop computer systems running in the Windows NT or Unix operating system environments. These state-of-the-art computer systems are loaded with approved Army auditing tools to perform appropriate diagnostic testing of installation networks.

CDAP Team Support Requirements

ACERT/CDAP Team requirements from a supported command or activity include the supported IP address range and continuous access to the activity/command internal LAN and NIPRNET/SIPRNET during the period of operational support. Other assistance and/or accommodations needed for the team include:

- Description and drawings of the command or activity network architecture(s);
- Identification of operating systems and versions;
- Identification of network perimeter defenses, i.e., firewalls, security routers, and/or intrusion detection systems;
- Administrative/security audit tools that are being utilized by network/system administrators or Information System Security Managers to monitor security;
- Command or activity information system security policy;
- Telephone number range if dial-up services are utilized;
- Identity of, and introduction to, unit Automation Section POCs;
- Local living accommodations and information regarding the area; and
- Assistance in ensuring on-site security for team personnel and material.

The ACERT maintains, analyzes and disseminates information concerning threats, vulnerabilities and incidents, and maintains a web page with AIS security-related information. For more information on the ACERT/CC, call the Chief, ACERT/CC Division at DSN 235-1113 (commercial 1-888-203-6332). For more information on the CDAP, call the CDA Branch Chief at DSN 235-2987 (commercial 703-706-2987). For more information about any of the four RCERTs listed above, call the RCERT Branch Chief at DSN 235-1192 (commercial 703-706-1192).

E. VULNERABILITY ASSESSMENT

The LIWA's IO Vulnerability Assessment Teams (IOVATs) are designed to assess and enhance an Army commander's ability to incorporate defensive IO (DIO) in his/her operational missions. When requested, a VAT is deployed to a location(s) to assess and identify vulnerabilities across the full spectrum of the command's information infrastructure. The team makes recommendations to mitigate command vulnerabilities and to introduce efficiencies to enhance the commander's warfighting capabilities in an information-rich environment. Vulnerability assessments employ both *"Blue"* and *"Red" Teams* to perform the VA missions.

VA Blue Team

The LIWA VA Blue Team, when deployed, plans and conducts *non-intrusive* assessments within the IO disciplines, focusing on information and network flow analyses and survey activities. All available information is assimilated to identify existing or potential vulnerabilities to adversary action, estimate the associated level of risk and recommend measures to diminish or eliminate the risk.

VA Blue Team Composition and Capabilities

A VA Blue Team normally is led by a Team Leader (MAJ) who acts as the spokesperson for the team and coordinates with the leadership of the assessed unit and other supporting elements (e. g., COMSEC monitoring team or LIWA FST, if employed). The team is rounded-out with up to five individuals (military, Government civilian or contractor) with skills and experience in information systems architectures; communications, computer and information systems security; EW; intelligence; and multi-discipline counterintelligence.

The VA Blue Team also offers assistance in evaluating a command's ability to exploit or influence the information environment, and assessing the resultant impact on the command's mission effectiveness. All disciplines ("pillars") of IO are generally considered, unless the assessed unit's commander specifically requests the omission of selected IO-oriented interests. Normally, an assessment will also include an analysis of the unit's information flow infrastructure and decision-making cycle to identify choke points or potential conflicts within the decision-making process.

As depicted in Figure 2, the VA Blue Team assessment process focuses on the command and control elements that affect the decision process.

The scope of the IOVA can be adapted to the particular unit and/or operation or mission on a case-by-case basis - dependent upon the commander's specific requirements and the operational environment. Assistance may include on-the-spot training, if requested, as well as recommendations for improvements in the conduct of IO. An assessment addresses the following areas of potential vulnerability:

- Commander's decision-making process or information flow;
- Results of adversary employment of IO;
- Hostile intelligence and CI activities; and
- Command DIO programs.

A variety of methods can be employed to achieve the execution phase objectives. The automated software tools used in the technical portions of the VA Blue Team assessment are limited to those specifically agreed to during the pre-assessment coordination with the assessed unit commander. A brief overview of the most common tools and techniques is described below.

- *Flow analysis* - Includes both information flow (mapping of the decision-making process within the unit and the required information flow to achieve effective results from that process) and network flow (in-depth look at the unit's automated structure which supports the information flow).
- *Verification* - Covers confirmation of the information gathered during pre-assessment; includes such areas as the unit's critical information, primary and back-up AIS connectivity; automated security measures in place, traditional security measures, training and awareness programs, coordination with supporting entities and internal controls.
- *Interview* - Allows team members to gather information on how the unit operates in the "real world", how policies and procedures are implemented, how effective existing measures are and how operators believe the unit functions could be improved.
- *Observation* - Verifies information extracted from flow analyses, and also confirms information obtained during interviews or in pre-assessment.
- *OPSEC analysis* - Identifies indicators and other observables which have the potential to reveal critical information associated with the unit or operation.
    - *Documentation review* - Covers a variety of documentation to ensure that unit policies and procedures are adequately documented.

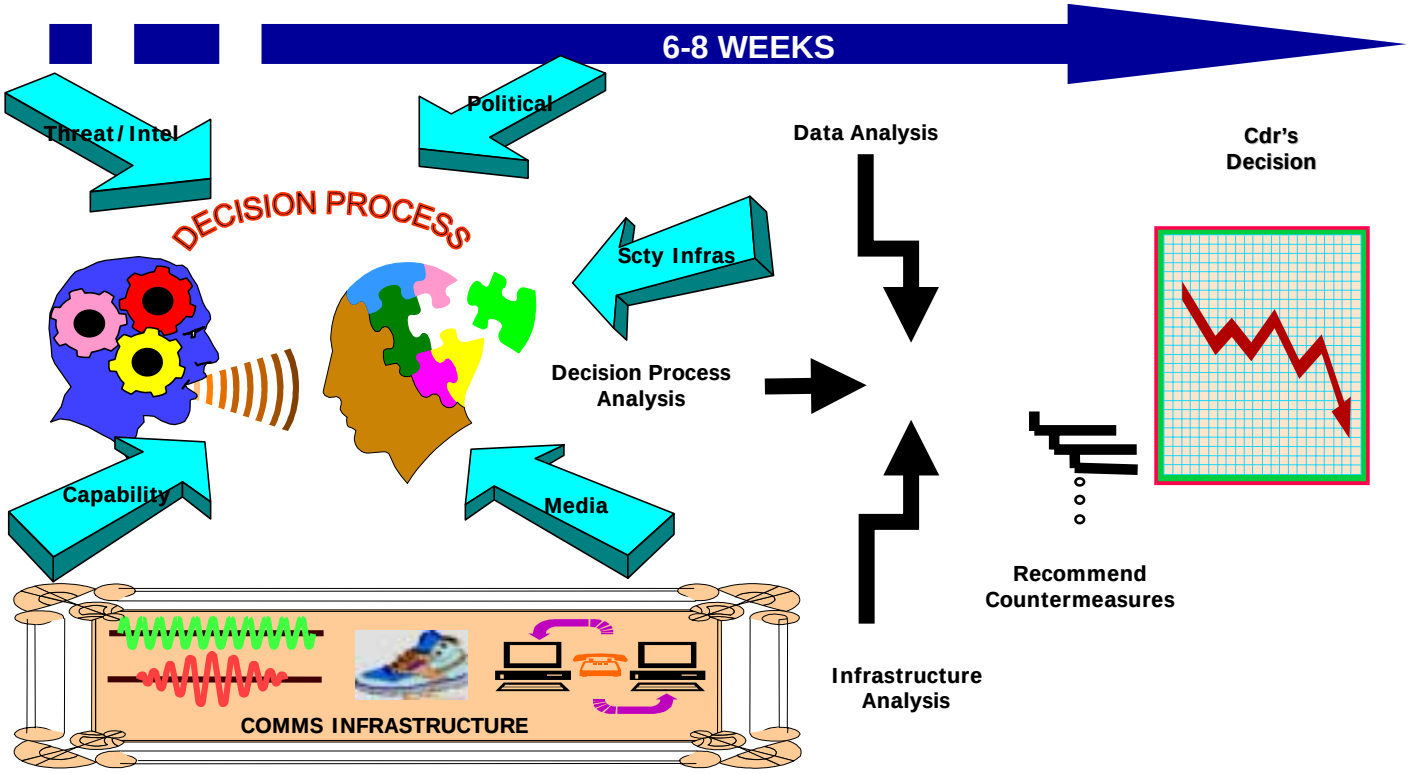

Figure 2. VA Blue Team Assessment Process

- *System review* - Establishes that proper procedures are being followed, (including back-up) are available, appropriate redundancy exists, proper AIS security measures are effectively observed and personnel are well-trained and skilled; and is performed at all levels of the assessed unit's automated systems.

VA Blue Team Support Requirements

To perform its assessment mission, the VA Blue Team requires support in the following areas:

- Access to command points of contact within the assessed areas of concentration;
- Workspace for up to four individuals;
- Access to Class "A" (or equivalent) unclassified and classified telephone service in the assessed command's main network/systems control facility for each shift of operations; and
- Copies of command policy and security documents, OPSEC plan and EEFI, physical security plan and command organizational diagram.

To be most effective, the VA Blue Team requires assessed command IP address range and continuous access to the command's internal, LAN and NIPRNET/SIPRNET during the assessment period. Other accommodations needed for the VA Blue Team include:

- Description and drawings of the command's network architecture(s);
- Identification of operating systems and versions;
- Legitimate user accounts (needed to conduct insider threat simulation);
- Telephone number range if dial-up services are utilized;
- Identity of, and introduction to, unit Automation Section POCs;

- Local living accommodations (possibly including tactical facilities and services, e. g., messing and transportation, depending upon environment);
- Local security protection for team equipment, classified material and weapons, as required; and
- When required, local facilities, equipment and material needed to support the conduct of IO training for command personnel by the LIWA personnel.

VA Red Team

The LIWA VA Red Team mission is essentially ***readiness assessment and training*** - simulating adversary capabilities targeted against a unit's information, information systems and decision-making cycle. The VA Red Team operations are designed to provide positive feedback to strengthen a unit's defensive IO posture, and are not intended to alienate, antagonize or threaten any individual or produce disparaging unit "report cards".

VA Red Team Composition and Capabilities

Effective VA Red Team operations require coordinated intelligence support, OPSEC, PSYOP, deception, EW, destruction (simulated), and other IO-associated capabilities like CA and PA to provide the optimal capability to discern and exploit a unit's vulnerabilities to hostile IO. The Red Team is task-organized to meet customer needs and is structured around the nature of the assessed unit's information systems, the adversary commander's decision-making cycle under analysis and operational requirements.

The team normally is led by a Team Leader (military officer/Government civilian) who acts as the spokesperson for the team and coordinates with the leadership of the assessed unit and other supporting elements (e. g., LIWA FST, if employed). With its leader, the team is composed of three to five individuals (military, Government civilian or contractor) with skills and experience much like those found in the VA Blue Team. The team will also possess other, stronger skills in the technical parameters of adversary information databases.

Red Team operations serve to support DIO by testing a unit's own protective capability. The Red Team functions generally consist of:

- Conducting technical penetration of information systems to assess real-world vulnerabilities;
- Employing "Computer Red Team" tools and techniques that would be available to a reasonably knowledgeable adversary;
- Simulating, using technical and non-technical methods, plausible adversary activities in the gathering and analysis of information;
- Assessing the operational impact of the information gathered if it was made available to an adversary; and
- Presenting a summary of information gathered by using simulated adversary techniques.

The duration and other parameters of a VA Red Team mission are normally defined by MOU between the assessed unit and the Director, LIWA during pre-assessment. The team conducts planned tests/exercises and demonstrations on a non- or minimal-interference (defined as realistic exercise play [e. g., active jamming of communications and/or non-communications devices]) basis. The Red Team mission is conducted in coordination with the supported commander to demonstrate vulnerabilities in such a manner as to be non-intrusive or non-destructive.

VA Red Team Support Requirements

The scope of VA Red Team operations may be limited by the legal boundaries imposed by public law and Army regulations and policy. In addition, the assessed unit commander may impose operational limitations on Red Team operations out of regard for safety and privacy.

To best perform its assessment mission, the VA Red Team requires virtually the same level of access and support needed by the VA Blue Team. Critical, additional arrangements to facilitate Red Team operations include:

- Formal request from the commander of the supported unit which meets the requirements of legal review;
- Identification of and access to an assessed command trusted agent to work with the team to ensure consideration of safety, security and exercise objectives; and
- Designation of and access to the command or exercise decision-makers via a formal or *ad hoc* "IO White Cell". (Blue and Red Teams may work in concert or independently with different roles in the VA mission.)

The VA Division of the LIWA may be called for more information on the VA Blue and Red Teams at DSN 235-1210/-1472 (commercial 703-706-1210/-1472).

F. REPROGRAMMING ANALYSIS

The LIWA Army Reprogramming Analysis Team - Threat Analysis (ARAT-TA) is responsible for preparing the mission data set requirements to facilitate the rapid ARAT-TA reprogramming of Army target sensing systems and Army aviation self- protection systems. The ARAT-TA monitors worldwide threat signatures to detect threat changes that affect target sensors in Army aircraft and other weapons systems. The team maintains direct communications with National-level intelligence agencies, scientific and technical intelligence centers and joint/Service reprogramming centers, in support of the rapid reprogramming effort.

For information on emergency reprogramming of Army electronic sensor systems, call the LIWA ARAT-TA Program Manager at DSN 235-1819 (commercial 703-706-1819).

G. LIWA SUPPORT SYNERGY

Figure 3, below, depicts the potential synergy among the IOVA Blue/Red teams and other LIWA support elements. An assessment might be set up to consist of separate Blue and Red Team missions, or one mission combining the two teams. Generally, when conducted in coordination with a Blue Team assessment, Red Team operations can independently validate vulnerabilities by challenging the assessed unit with a "real", adversary-like action. The VA team(s) also might be deployed to conduct their VA mission(s) preceding or coincident with a LIWA FST deployment, or in conjunction with an ACERT/CDAP assessment.

Refer to the LIWA Deputy Director for Operations, DSN 235-2262 (commercial 703-706-2262) for more information on combining multiple LIWA missions.

III. REQUESTS FOR LIWA SUPPORT

The LIWA is assigned to Headquarters, U. S. Army INSCOM. *Operational control* over LIWA activities is vested in the Information Operations Division of the Operations, Readiness and Mobilization Directorate (message address: *DAMO-ODI*) in the ODCSOPS, HQDA.

The initial request for support from the LIWA should be submitted via message (see Figure 4 (LIWA Tasking Message Format), below, specifying the support required and the inclusive dates. Direct liaison between the LIWA and the requesting headquarters is encouraged by HQDA.

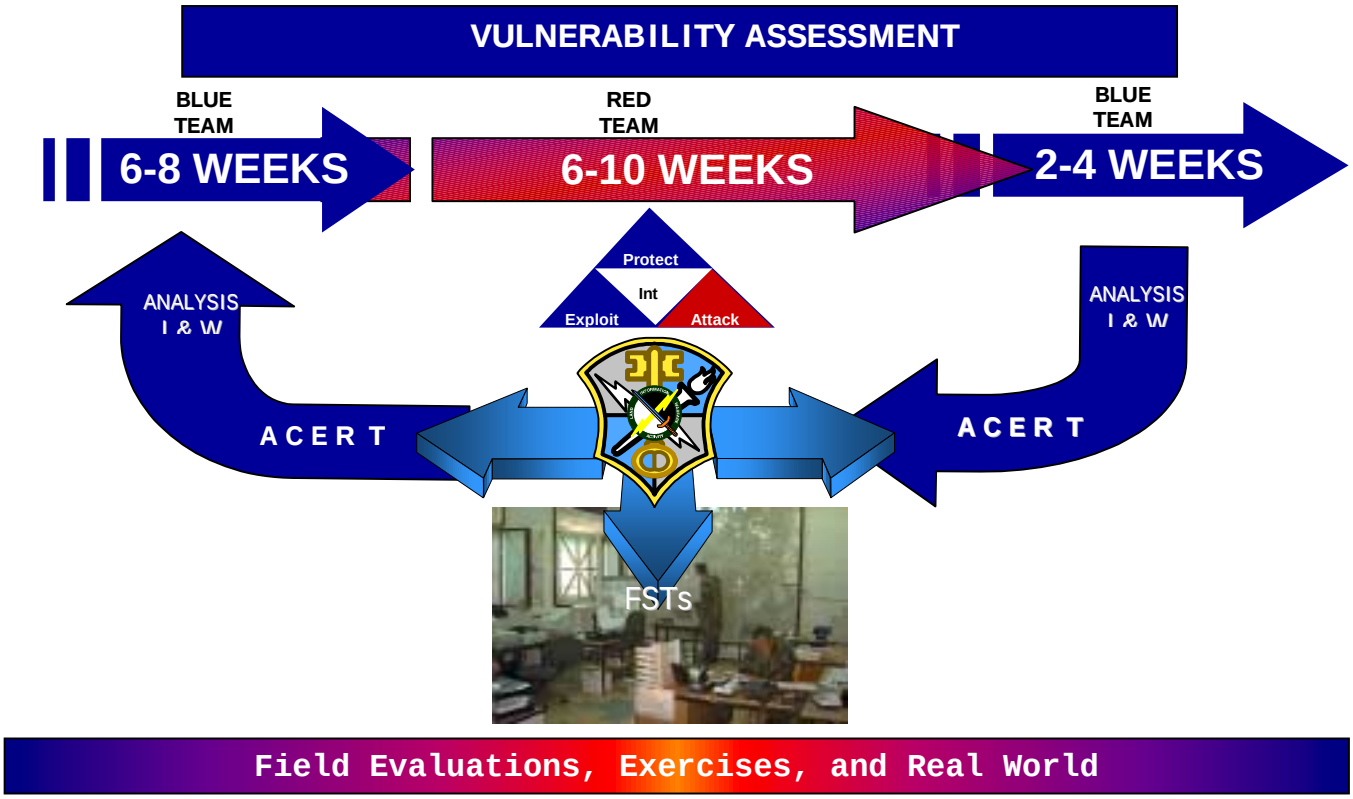

Figure 3. LIWA IO Support Synergy

It should be noted, however, that the LIWA is not sufficiently funded to cover the expense of supporting all Army IO missions. Units or organizations considering LIWA support are advised to plan ahead for funding the use of LIWA resources and be prepared to share travel and per diem costs for LIWA participation.

LIWA TASKING MESSAGE FORMAT

FM (REQUESTING COMMAND)
TO DA WASHINGTON DC//DAMO-ODI//
DIRLIWA FT BELVOIR VA//DO//
INFO (REQUESTOR'S CHOICE)
CDRINSCOM FT BELVOIR VA//IAOP//
SUBJ: REQUEST FOR LIWA SUPPORT

1. REQUEST LIWA SUPPORT FOR *(EXERCISE OR OPERATION)* DURING THE PERIOD (INCLUSIVE DATES). LIWA SUPPORT IS REQUIRED TO PROVIDE *(INDICATE SPECIFIC TYPE OF SUPPORT REQUIRED, E.G., FIELD SUPPORT AUGMENTATION, RED TEAMING, VULNERABILITY ASSESSMENT, COMPUTER EMERGENCY RESPONSE, COMPUTER DEFENSE ASSISTANCE, ETC).* ALSO INDICATE ANY SPECIAL REQUIREMENTS OR LIMITATIONS ASSOCIATED WITH THE REQUESTED SUPPORT.
2. FUND CITE FOR LIWA PARTICIPATION WILL BE PROVIDED BY SEPARATE CORRESPONDENCE WHEN MISSION IS APPROVED. RESOURCE MANAGEMENT POC IS *(NAME, GRADE, POSITION, OFFICE) AT (COMMERCIAL AND DSN TELEPHONE/FAX NUMBERS AND NIPRNET/SIPRNET/JWICS E-MAIL ADDRESSES).*
3. REQUEST DIRECT LIAISON BE AUTHORIZED BETWEEN DIRLIWA AND THIS HEADQUARTERS.
4. DIRLIWA WILL BE ADDED TO MESSAGE ADDRESSEE LIST FOR ALL APPROPRIATE *(EXERCISE/OPERATIONAL)* MESSAGE TRAFFIC *(INCLUDE GENSER, DSSCS, SPECAT AND SAR MESSAGE TRAFFIC, AS APPROPRIATE).*
5. POC FOR THIS ACTION IS *(NAME, GRADE, POSITION, OFFICE)* AT *(PROVIDE COMMERCIAL AND DSN TELEPHONE/FAX NUMBERS AND NIPRNET/SIPRNET/JWICS E-MAIL ADDRESSES, AS APPROPRIATE).*

Figure 4. LIWA Tasking Message Format

NOTE TO THE USER

This guide or any part thereof may be reproduced and distributed, as needed. The user should be aware that current doctrine for information operations in the military information environment is undergoing a widespread review prior to significant revision. The revision, for the most part, will reflect the tactics, techniques and procedures reported by the LIWA from experience gained in over 50 field exercises, experiments and contingency, real-world deployments.